pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Proper Use and Disclosure of Personally Identifiable Information (PII)

Number
ITP-SEC025

Effective Date
March 19, 2010

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
April 2024

1. Purpose

This Information Technology Policy (ITP) provides guidelines for the exercise of agency discretion in creating policies and procedures on the proper electronic use and disclosure of Personally Identifiable Information (PII).

It is important for an agency to recognize that non-PII can become PII whenever additional information is made available that, when combined with other available information, could be used to identify an individual.

Examples of PII include, but are not limited to, any combination of the following personally identifiable attributes:

- Name
- Date and place of birth
- Mother's maiden name
- Biometric records
- Social Security Number
- Driver's license number or a state identification card number, in lieu of a driver's license
- Passport Number
- Financial account number, credit or debit card number, in combination with any required security code, access code or password
- Medical information
- Health insurance information, policy or subscriber identification number in combination with access code or other medical information
- Username or email address, in combination with a password or security question and answer

Agencies may have additional attributes beyond those stated above they are required to protect under certain policies, laws, or regulations (i.e., Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information

Services (CJIS), or Internal Revenue Service (IRS)) that are specific to their agency or type of data handled.

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Policy

The Office of Administration/Office for Information Technology (OA/IT) is committed to protecting the privacy of PII of its employees, contractors, constituents, and other individuals associated with the Commonwealth. All agencies shall take appropriate measures, implement necessary technology, and establish operating procedures to ensure data privacy is maintained. All applications collecting PII must comply with applicable laws and be vetted through the CA2 process (detailed in *ITP-SEC005, Commonwealth Application Certification and Accreditation).*

Identifying PII

Agencies are responsible for identifying and classifying all PII generated, collected, stored, used, and disclosed by the agency or by a third-party on the agency's behalf. This data includes Sensitive Security Information, Protected Information, Privileged Information and Prerequisite-required information. Refer to *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data* for data classification guidance.

Collecting PII

Agencies shall limit the generation, collection, storage, use, and disclosure of PII to that which is necessary for business purposes only and shall further limit generation, collection, storage, use, and disclosure of PII to the ***minimum*** extent necessary for the accomplishment of those business purposes.

Systems which are vendor or agency hosted shall use PII as data elements only and not as keys to databases. PII may be used for identification purposes or as identifiers only to address a business necessity, and only if allowed by applicable law, regulations or mandates.

Displaying PII

Systems which are vendor or agency hosted shall not display PII visually, whether on computer monitors, or on printed forms, or other system output, unless required by any law or other requirement applicable to an agency, or business necessity.

PII in Test Environments

PII data shall not be used in staging, development, or test environments (non-production environments). Simulated PII data shall be utilized in these environments.

Unique Identifiers

Systems developed by an agency, third-party, contracted provider, or business partner

that require a unique identifier shall not use PII as that identifier. All systems, which must assign an identifying number for an individual, must assign a unique identification number that is not the same as, or cannot be traced back to users PII. Security must be applied, and care must be taken to ensure that access to the electronic system and use of these unique identification numbers are restricted in accordance with any law or other requirement applicable to an agency.

Transferring PII

PII moved from one computer to another shall be transferred using encryption controls defined in *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data* and *ITP-SEC031, Encryption Standards* to protect data integrity and confidentiality. Agency legal review may be required, and is otherwise recommended, to ensure appropriate limits and processes are applied to any PII data transfer between Commonwealth agencies, business partners, or external entities.

Maintaining PII

All agencies maintaining files utilizing PII for any purpose shall ensure that access or use of such information is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure and that the retention period is minimized based upon business requirements.

Legacy Systems

Owners of legacy information systems that use PII as keys or indexes in their databases and which are not specifically required to do so by any law, regulation, reporting requirement or other mandate shall have an action plan and timelinefor remediation.

Disclosure of PII

Security Incidents involving PII must be reported via the requirements outlined in *ITP-SEC024, IT Security Incident Reporting Policy* regardless of other law or requirements that may be applicable to security incidents or Data Breaches. Security incidents, for reporting under ITP-SEC024, include loss or compromise of data in electronic or paper form. Good faith acquisition of personal information by an authorized user for the purposes of Commonwealth business is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of Commonwealth business and is not subject to further unauthorized disclosure. Agencies or business partners shall follow all laws applicable to the security incident and agency requirements.

4. Responsibilities

4.1 Agencies shall:

Comply with the requirements as outlined in this ITP and ensure that all users of agency systems are aware of the procedures and importance of reporting security incidents (refer to ITP-SEC024 for guidance), Security incidents, threats, or malfunctions may have an impact on the security of agency information.

4.2 OA/IT shall:

Comply with the requirements as outlined in this ITP.

4.3 Third-party vendors, licensors, contractors, or suppliers shall:

- Perform a data element inventory, identifying and classifying all PII generated, collected, stored, used, and disclosed by the third-party on the agency's behalf.
- Ensure that access or use of information utilizing PII, or other protected data types (CJIS, FTI, HIPAA) for any purpose, is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure. For Social Security Administration (SSA) compliance, the system's encryption methods must align with the guidelines established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standards (AES) or Triple Data Encryption Algorithm (Triple DES).
- Take appropriate measures, implement necessary technology, and establish operating procedures to ensure data privacy is maintained.
- Limit the generation, collection, storage, use, and disclosure of PII to that which is necessary for business purposes only.
- Ensure that systems that require a unique identifier do not use PII as that identifier.
- Assign a unique identification number to an individual for systems requiring it. The unique identification number cannot be the same as or cannot be traced back to the users PII. Security must be applied, and care must be taken to ensure that access to the electronic system and use of these unique identification numbers are restricted in accordance with any applicable law or other agency requirement.
- Ensure contractor and agency hosted systems do not display PII visually, whether on computer monitors, or on printed forms, or other system outputs, unless required by any applicable law or other agency requirement.
- Ensure security incidents involved PII are reports following *ITP-SEC024, IT Security Incident Reporting Policy* in addition to any other laws or regulations for incidents or data breaches, such as the Breach of Personal Information Notification Act.
- Obtain approval from the contracting agency and the Office of Administration before using cloud storage.

5. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/Glossary.aspx*
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *ITP-PRV001, Commonwealth of PA Electronic Information Privacy Policy*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC005, Commonwealth Application Certification and Accreditation*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC024, IT Security Incident Reporting Policy*

- *ITP-SEC031, Encryption Standards*
- NIST SP 800-122 - *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- *Breach of Personal Information Notification Act, as amended November 3, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301-2330*
- *HIPAA regulations*
- *Sarbanes Oxley Act of 2002*
- *Payment Card Industry Standards*

6. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

7. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

8. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to Commonwealth users only.

Version	Date	Purpose of Revision	Redline Link
Original	3/19/2010	Base Document	N/A
Revision	05/17/2011	Changed ITB # from 36 to 25	N/A
Revision	10/07/2011	Policy updated to reflect EASC comments	N/A
Revision	04/20/2012	Policy updated to reflect OA-Legal comments	N/A
Revision	04/02/2014	ITP Reformat	N/A
Revision	01/12/2018	Added Definitions and Exemption from Policy section Revised Policy opening statement	N/A
Revision	11/03/2021	• Updated purpose to include examples of PII • Added offices and third-party vendors to scope • Updated definitions • Updated and add links to policy references • Added Responsibilities section • Updated Related ITPs/Other References section • Updated Exemption language	N/A
Revision	4/07/2023	• Additional attributes added to examples of PII under Purpose • Scope expanded consistent with other Security ITPs • References added/updated to ITP-INF015 where appropriate	Revised IT Policy Redline <04/07/2023>

Version	Date	Purpose of Revision	Redline Link
		• Reference added to ITP-SEC031 under Transferring PII • Additional guidance added under Disclosure of PII in relation to good faith acquisitions by authorized users • Act 151 added as reference	